Attorney Docket No. 1391.1049

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Daiji SANAI et al.

Application No.: Unassigned | Group Art Unit: Unassigned

Filed: October 3, 2003 | Examiner: Unassigned

For: PASSWORD STRENGTH CHECKING METHOD AND APPARATUS AND PROGRAM AND RECORDING MEDIUM....

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicant(s) submit(s) herewith a certified copy of the following foreign application:

Japanese Patent Application No(s). 2002-298190, 2002-366243 and 2002-366258

Filed: October 11, 2002 and December 18, 2002

It is respectfully requested that the applicant(s) be given the benefit of the foreign filing date(s) as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,

STAAS & HALSEY LLP

Date: October 3, 2003 By: David M. Pitcher

David M. Pitcher
Registration No. 25,908

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年１０月１１日

出願番号
Application Number: 特願２００２－２９８１９０

[ST.10/C]: [ＪＰ２００２－２９８１９０]

出願人
Applicant(s): 株式会社山武

２００３年　７月　４日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０５３４６６

【書類名】　特許願
【整理番号】　20020259
【提出日】　平成14年10月11日
【あて先】　特許庁長官殿
【国際特許分類】　G06F 17/00
【発明者】
【住所又は居所】　東京都渋谷区渋谷２丁目１２番１９号　株式会社　山武内
【氏名】　三島　崇
【発明者】
【住所又は居所】　東京都渋谷区渋谷２丁目１２番１９号　株式会社　山武内
【氏名】　関　英信
【発明者】
【住所又は居所】　東京都渋谷区渋谷２丁目１２番１９号　株式会社　山武内
【氏名】　有元　伯治
【発明者】
【住所又は居所】　東京都渋谷区渋谷２丁目１２番１９号　株式会社　山武内
【氏名】　佐内　大司
【特許出願人】
【識別番号】　000006666
【氏名又は名称】　株式会社　山武
【代理人】
【識別番号】　100095072
【弁理士】
【氏名又は名称】　岡田　光由
【電話番号】　03-3807-1818

【手数料の表示】

【予納台帳番号】　012944

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9722522

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　パスワード強度検査方法及びその装置と、パスワード強度検査プログラム及びそのプログラムを記録した記録媒体

【特許請求の範囲】

【請求項１】　検査対象のパスワードを入力する過程と、

パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパスワード候補を生成する過程と、

上記入力したパスワードと上記生成したパスワード候補とが一致するのか否かを判断する過程と、

上記一致を判断しない場合に、次のパスワード候補の生成を指示する過程と、

上記一致を判断する場合に、上記生成したパスワード候補の個数に従って、上記入力したパスワードの強度を決定する過程と、

上記決定したパスワード強度の情報を出力する過程とを備えることを、

特徴とするパスワード強度検査方法。

【請求項２】　請求項１記載のパスワード強度検査方法において、

上記入力する過程では、ユーザに見えないような形でパスワードの入力状態をユーザに提示しつつ、ユーザに対して、再度パスワードの入力を要求して、その入力した２つのパスワードが一致することを条件にして、検査対象のパスワードを入力することを、

特徴とするパスワード強度検査方法。

【請求項３】　請求項１又は２記載のパスワード強度検査方法において、

上記入力する過程では、ユーザの属性情報についても入力して、その入力したユーザの属性情報と上記入力したパスワードとが一致する場合には、その入力したパスワードの強度検査に入らないように制御することを、

特徴とするパスワード強度検査方法。

【請求項４】　請求項１ないし３のいずれか１項に記載のパスワード強度検査方法において、

上記決定する過程では、上記生成したパスワード候補の個数に従って、上記パスワード推測ツールが検査対象のパスワードを攻撃する場合に要する攻撃時間を

推定して、それをパスワード強度として決定することを、

特徴とするパスワード強度検査方法。

【請求項５】　請求項１ないし３のいずれか１項に記載のパスワード強度検査方法において、

上記決定する過程では、上記パスワード候補の最大可能な生成個数と上記生成したパスワード候補の個数との比率値に応じて算出される数値情報を算出して、それをパスワード強度として決定することを、

特徴とするパスワード強度検査方法。

【請求項６】　請求項１ないし５のいずれか１項に記載のパスワード強度検査方法において、

上記出力する過程では、更に、上記決定したパスワード強度により特定されることになるこれまでにパスワード強度を決定した検査対象のパスワードの中における順位情報についても出力することを、

特徴とするパスワード強度検査方法。

【請求項７】　検査対象のパスワードを入力する手段と、

パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパスワード候補を生成する手段と、

上記入力したパスワードと上記生成したパスワード候補とが一致するのか否かを判断する手段と、

上記一致を判断しない場合に、次のパスワード候補の生成を指示する手段と、

上記一致を判断する場合に、上記生成したパスワード候補の個数に従って、上記入力したパスワードの強度を決定する手段と、

上記決定したパスワード強度の情報を出力する手段とを備えることを、

特徴とするパスワード強度検査装置。

【請求項８】　検査対象のパスワードを入力する処理と、

パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパスワード候補を生成する処理と、

上記入力したパスワードと上記生成したパスワード候補とが一致するのか否かを判断する処理と、

上記一致を判断しない場合に、次のパスワード候補の生成を指示する処理と、

上記一致を判断する場合に、上記生成したパスワード候補の個数に従って、上記入力したパスワードの強度を決定する処理と、

上記決定したパスワード強度の情報を出力する処理とをコンピュータに実行させるためのパスワード強度検査プログラム。

【請求項９】　検査対象のパスワードを入力する処理と、

パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパスワード候補を生成する処理と、

上記入力したパスワードと上記生成したパスワード候補とが一致するのか否かを判断する処理と、

上記一致を判断しない場合に、次のパスワード候補の生成を指示する処理と、

上記一致を判断する場合に、上記生成したパスワード候補の個数に従って、上記入力したパスワードの強度を決定する処理と、

上記決定したパスワード強度の情報を出力する処理とをコンピュータに実行させるためのパスワード強度検査プログラムを記録した記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、パスワードの強度を検査するパスワード強度検査方法及びその装置と、そのパスワード強度検査方法の実現に用いられるパスワード強度検査プログラム及びそのプログラムを記録した記録媒体とに関する。

【０００２】

【従来の技術】

ユーザがコンピュータ上で動作するシステムを利用する場合には、ユーザに対して、予めコンピュータに登録させたパスワードと同一のパスワードを入力させるようにすることで、ユーザがシステムを利用できる本人であるのか否かを確認するようにしている。

【０００３】

コンピュータに登録されるパスワードは、盗まれる可能性があることから暗号

化されており、これから、システムの利用時にユーザから平文のパスワードが入力されると、それを暗号化して、この登録されている暗号化パスワードと一致するのか否かを判断することで、ユーザがシステムを利用できる本人であるのか否かを確認するようにしている。

【０００４】

コンピュータに登録されるパスワードは、通常の場合、セキュリティを確保するために、一方向性を有する暗号化方式（暗号化されたものを平文に戻すことが難しい暗号化方式）を使って暗号化されており、これから、悪意のあるユーザは、コンピュータに登録されている暗号化パスワードを入手すると、「Ｊohn the Ripper」などのようなパスワード推測ツールを使って、ブルートフォースと呼ばれる攻撃を実行することで、その暗号化パスワードに対応付けられる平文のパスワードを盗み取るようにしている（例えば、非特許文献１参照）。

【０００５】

すなわち、図９に示すように、パスワードとして使用できるすべての文字を組み合わせることで平文のパスワード候補を生成して、それを暗号化（ハッシュ化）したものがコンピュータに登録されている暗号化パスワードと一致するのか否か判断することを繰り返していくブルートフォースと呼ばれる攻撃を実行することで、その暗号化パスワードに対応付けられる平文のパスワードを盗み取るようにしているのである。

【０００６】

なお、このブルートフォースは、例えば、ユーザがパスワードを忘れてしまったような場合に、そのパスワードを得るために実行されることもある。

【０００７】

【非特許文献１】

三島など：“ブルートフォースに勝つ“強いパスワード”とは”，日経ネットワークセキュリティ，Vol.2,pp.36-47(2002).

【０００８】

【発明が解決しようとする課題】

セキュリティを確保するためには、強いパスワードを付けることが必須である

。しかしながら、現在、どのようなパスワードを使えば強いと言えるのか明確な指標はない。

【０００９】

これから、ユーザは、どのようなパスワードを付ければよいのかよく分からないというのが実情である。「長いパスワードを使う」とか、「英数字記号を混ぜる」などのアドバイスがあるものの、実際に、どのようなパスワードを付ければよいのかよく分からないというのが実情である。

【００１０】

悪意のあるユーザにパスワードを盗まれないようにするためには、ブルートフォースの攻撃に対して、短い時間で解答の平文パスワードが得られないようにしていく必要がある。

【００１１】

そこで、パスワード推測ツールを使ったブルートフォースの攻撃を受けたときに、パスワードが盗み取られるまでの時間を測定して、それをパスワードの強度として用いるということが考えられる。

【００１２】

このようにして定義されるパスワードの強度はセキュリティの高さを示していることから適切であるものの、パスワード推測ツールを使ったブルートフォースの攻撃では、パスワードとして使用できる文字の組み合わせが天文学的な数値となり、更にそれを暗号化する必要があることで、そのパスワードの強度が求まるまでに数カ月も要するということが起こり実際には採用することができない。

【００１３】

このように、従来技術では、パスワードの強度を数値的に表現することが提供されておらず、これがために、ユーザは、自分が強いと考えるパスワードを付けるしかなかった。

【００１４】

本発明はかかる事情に鑑みてなされたものであって、実用的な時間内で数値的に表現されるパスワードの強度を算出できるようにすることで、パスワードの強度を客観的かつ正確に検査できるようにする新たなパスワード強度検査技術の提

供を目的とする。

【００１５】

【課題を解決するための手段】

この目的を達成するために、本発明のパスワード強度検査装置は、パスワードの強度を検査することを実現するために、①検査対象のパスワードを入力する入力手段と、②パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパスワード候補を生成する生成手段と、③入力手段の入力したパスワードと生成手段の生成したパスワード候補とが一致するのか否かを判断する判断手段と、④判断手段が一致を判断しない場合に、生成手段に対して、次のパスワード候補の生成を指示する指示手段と、⑤判断手段が一致を判断する場合に、生成手段の生成したパスワード候補の個数に従って、入力手段の入力したパスワードの強度を決定する決定手段と、⑥決定手段の決定したパスワード強度の情報を出力する出力手段とを備えるように構成する。

【００１６】

以上の各処理手段が動作することにより実現される本発明のパスワード強度検査方法はコンピュータプログラムで実現できるものであり、このコンピュータプログラムは、半導体メモリなどのような適当な記録媒体に記録して提供することができる。

【００１７】

このように構成される本発明のパスワード強度検査装置では、検査対象のパスワードを入力すると、パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパスワード候補を生成して、その入力したパスワードとその生成したパスワード候補とが一致するのか否かを判断する。

【００１８】

そして、この一致を判断しない場合には、次のパスワード候補の生成を指示することで、入力したパスワードと生成したパスワード候補とが一致することになるまで、次々とパスワード候補を生成していく。

【００１９】

一方、この一致を判断する場合には、生成したパスワード候補の個数に従って

、例えば、パスワード推測ツールが入力したパスワードを攻撃する場合に要する攻撃時間を推定して、それを入力したパスワードの強度として決定したり、パスワード候補の最大可能な生成個数と生成したパスワード候補の個数との比率値に応じて算出される数値情報を算出して、それを入力したパスワードの強度として決定することにより、入力したパスワードの強度を決定して、その決定したパスワード強度の情報を出力する。

【００２０】

このとき、決定したパスワード強度の情報の出力に加えて、その決定したパスワード強度により特定されることになる、これまでにパスワード強度を決定した検査対象のパスワードの中における順位情報についても出力することがある。

【００２１】

この構成を採るときにあって、パスワードとしての性質を持たないパスワードが検査対象となっても意味がないことから、そのようなパスワードの検査を排除すべく、ユーザに見えないような形でパスワードの入力状態をユーザに提示しつつ、ユーザに対して、再度パスワードの入力を要求して、その入力した２つのパスワードが一致することを条件にして、検査対象のパスワードを入力するように処理することがある。

【００２２】

また、ユーザ属性と一致するパスワードについては極めて脆弱なパスワードであることを考慮して、パスワードの入力時に、電話番号などのようなユーザの属性情報についても入力するようにして、その入力したユーザの属性情報と入力したパスワードとが一致する場合には、その入力したパスワードの強度検査に入らないように制御するように処理することがある。

【００２３】

このように、本発明では、検査対象のパスワードがブルートフォースの攻撃で用いられるパスワード推測ツールで生成される平文のパスワード候補の何個目のパスワードに該当するのかということを測定して、その何個目という数に従ってパスワードの強度を決定して出力するという構成を採ることから、実用的な時間内で数値的に表現されるパスワードの強度を算出できるようになることで、パス

ワードの強度を客観的かつ正確に検査できるようになる。

【００２４】

【発明の実施の形態】

以下、実施の形態に従って本発明を詳細に説明する。

【００２５】

図１に、本発明のパスワード強度検査装置１の装置構成の一実施形態例を図示する。

【００２６】

この図に示す本発明のパスワード強度検査装置１は、例えば、ユーザに強いパスワードの付けかたを学習させるために使われるものであって、この図に示すように、ユーザとの対話手段となる入出力装置１０と、「Ｊohn the Ｒipper 」などのようなパスワード推測ツールで用いられて、平文のパスワード候補を生成するパスワード候補生成ルーチン１１と、そのパスワード候補生成ルーチン１１を使って、検査対象のパスワードの強度を検査するパスワード強度検査プログラム１２と、そのパスワード強度検査プログラム１２による検査結果を記録する順位テーブル１３とを備える。

【００２７】

このパスワード候補生成ルーチン１１は、後述する処理フローから分かるように、入出力装置１０から検査対象のパスワードを入力する機能と、パスワード候補生成ルーチン１１に対してパスワード候補の生成を依頼する機能と、入力したパスワードとパスワード候補生成ルーチン１１の生成したパスワード候補とが一致するのか否かを判断する機能と、パスワード候補生成ルーチン１１の生成したパスワードの個数に従って、入力したパスワードの強度を決定する機能と、決定したパスワード強度を出力する機能とを有する。

【００２８】

パスワード候補生成ルーチン１１は、「Ｊohn the Ｒipper 」などのようなパスワード推測ツールで用いられて、例えば、最初は、辞書に記載された文字列を使って平文のパスワード候補を生成し、続いて、パスワードとして使用できるすべての文字列を使って平文のパスワード候補を生成していくことで、７兆を超え

る平文のパスワード候補を規定の順番に従って生成するように処理する。

【００２９】

順位テーブル１３は、パスワード強度検査プログラム１２による検査結果を記録するものであって、図２に示すように、例えば、パスワード強度を示す得点（１００点が満点となる）の高い順に、これまでに検査したパスワードと、そのパスワードを入力したユーザ名と、そのパスワードの得点とを記録する。

【００３０】

図３及び図４に、パスワード強度検査プログラム１２の実行する処理フローの一実施形態例を図示する。

【００３１】

次に、この処理フローに従って、本発明によるパスワード強度の検査処理について詳細に説明する。

【００３２】

パスワード強度検査プログラム１２は、本発明のパスワード強度検査装置１の電源が投入されることで起動されると、図３及び図４の処理フローに示すように、先ず最初に、ステップ１で、順位テーブル１３をクリアする。

【００３３】

続いて、ステップ２で、入出力装置１０のディスプレイに、図５に示すようなパスワード検査画面を表示する。

【００３４】

この図５に示すように、パスワード検査画面は、「ユーザ名」の入力域と、「パスワード」の入力域と、「パスワード確認」と呼ばれるパスワードの入力域という３つの入力域を有するとともに、順位テーブル１３に記録される検査結果の情報（但し、パスワードについては除く）の表示域を有している。

【００３５】

なお、図中に示す「Ｃheckボタン」は、入力されたパスワードの検査の実行を指示するために用意され、「Ｒetry」ボタンは、「ユーザ名」に入力されたユーザ名については残したままで、「パスワード」及び「パスワード確認」に入力されたパスワードをクリアすることを指示するために用意され、「Ｎewボタン」は

、「ユーザ名」に入力されたユーザ名と「パスワード」及び「パスワード確認」に入力されたパスワードとをクリアすることを指示するために用意される。

【００３６】

このパスワード検査画面の表示に応答して、ユーザは、図６に示すように、「ユーザ名」の入力域にユーザ名を入力し、「パスワード」の入力域にパスワードを入力し、「パスワード確認」の入力域に「パスワード」の入力域に入力したパスワードと同一のパスワードを入力してから、「Ｃheckボタン」を操作することで、入力したパスワードの検査要求を発行してくる。

【００３７】

ここで、「パスワード」及び「パスワード確認」の入力域に入力されていくパスワードそのものについては表示せずに、“＊”のような記号を使って、その入力状態が分かるような表示方法を用いている。

【００３８】

これから、ステップ２でパスワード検査画面を表示すると、続くステップ３で、ユーザからパスワードの検査要求が発行されたのか否かを判断する。

【００３９】

この判断処理に従って、ユーザからパスワードの検査要求が発行されないことを判断するときには、ステップ４に進んで、ユーザから検査処理の終了要求が発行されたのか否かを判断して、ユーザから検査処理の終了要求が発行されたことを判断するときには、処理を終了し、ユーザから検査処理の終了要求が発行されないことを判断するときには、ステップ３に戻っていくことで、ユーザからパスワードの検査要求が発行されるのを待つ。

【００４０】

すなわち、ユーザがパスワードの検査処理を終了するときには、パスワード検査画面の持つ「終了ボタン」を操作してくるので、その「終了ボタン」が操作された場合には、ユーザから処理終了要求が発行されたことを判断して、処理を終了するのである。

【００４１】

一方、ステップ３で、ユーザからパスワードの検査要求が発行されたことを判

断するときには、ステップ５に進んで、「ユーザ名」の入力域に入力されたユーザ名と、「パスワード」の入力域に入力されたパスワードと、「パスワード確認」の入力域に入力されたパスワードとを抽出する。

【００４２】

続いて、ステップ６で、ステップ５で抽出した２つのパスワードが一致するのか否かを判断して、２つのパスワードが一致しないことを判断するときには、ステップ７に進んで、パスワード検査画面にパスワードの再入力を指示してから、ステップ３に戻っていくことで、ユーザからパスワードの検査要求が発行されるのを待つ。

【００４３】

すなわち、ユーザが「パスワード」の入力域と「パスワード確認」の入力域とに同一のパスワードを入力できないということは、ユーザが記憶不可能な文字列（パスワードとして使用できない文字列）であることが想定されるので、そのようなパスワードについては検査対象としないために、図７に示すように、パスワード検査画面にパスワードの再入力を指示してから、ステップ３に戻っていくことで、ユーザからパスワードの検査要求が発行されるのを待つのである。

【００４４】

一方、ステップ６で、ステップ５で抽出した２つのパスワードが一致することを判断するときには、ステップ８に進んで、ステップ５で抽出したユーザ名とステップ５で抽出したパスワードとが一致するのか否かを判断する。

【００４５】

この判断処理により、ステップ５で抽出したユーザ名とステップ５で抽出したパスワードとが一致することを判断するときには、ステップ９に進んで、パスワード検査画面に論外のパスワードであることを出力するとともに、パスワードの再入力を指示してから、ステップ３に戻っていくことで、ユーザからパスワードの検査要求が発行されるのを待つ。

【００４６】

すなわち、ユーザ名と一致するパスワードは簡単に盗まれることになるので、そのようなパスワードについては論外のパスワードであることを出力するととも

に、パスワードの再入力を指示してから、ステップ３に戻っていくことで、ユーザからパスワードの検査要求が発行されるのを待つのである。

【００４７】

一方、ステップ８で、ステップ５で抽出したユーザ名とステップ５で抽出したパスワードとが一致しないことを判断するときには、ステップ１０に進んで、パスワード候補生成ルーチン１１に対して、パスワード候補の生成を指示する。

【００４８】

このパスワード候補の生成指示を受け取ると、パスワード候補生成ルーチン１１は、パスワード推測ツールで用いられるときと同様の手順に従って、今回初めてパスワード候補を生成するときには、最初のパスワード候補（平文）を生成し、前回パスワード候補を生成しているときには、前回生成したパスワード候補に続くパスワード候補（平文）を１つ作成する。

【００４９】

これから、続いて、ステップ１１で、パスワード候補生成ルーチン１１から、その生成されたパスワード候補を受け取り、続くステップ１２で、入力したパスワード（ステップ５で抽出したパスワード）とその受け取ったパスワード候補とが一致するのか否かを判断する。

【００５０】

この判断処理により、入力したパスワードとパスワード候補生成ルーチン１１から受け取ったパスワード候補とが一致することを判断するときには、ステップ１３に進んで、その一致が得られるまでにパスワード候補生成ルーチン１１が生成したパスワード候補の個数と、パスワード候補生成ルーチン１１が最大生成可能とするパスワード候補の個数との比率値ｔ（０≦ｔ≦１）

ｔ＝（パスワード候補生成個数）／（パスワード候補最大生成可能個数）

を算出する。

【００５１】

続いて、ステップ１４で、

得点＝１００×ｔ

の算出式に従って、入力したパスワードの強度を示す得点を算出し、続くステッ

プ１５で、

推定解析時間＝τ×（生成したパスワード候補の個数）

の算出式に従って、悪意のあるユーザがパスワード推測ツールを使って入力したパスワードをブルートフォース攻撃をしたときに要する解析時間を推定する。

【００５２】

ここで、τは、１個のパスワード候補を生成してハッシュ化し、それをブルートフォース攻撃対象の暗号化パスワードと比較して、両者が一致するのか否かを判断するまでの処理を行うのに要する時間を示している。

【００５３】

続いて、ステップ１６で、入力したパスワードを順位テーブル１３に登録することで、順位テーブル１３のテーブルデータを更新する。このとき、図２に示す順位テーブル１３のテーブルデータから分かるように、算出した得点に従ってソートする形で、入力したパスワードの情報（ユーザ名、得点、パスワード）を順位テーブル１３に登録することになる。

【００５４】

続いて、ステップ１７で、図８に示すように、パスワード検査画面に対して、算出した得点および推定解析時間を出力するとともに、順位テーブル１３の情報を出力してから、次のパスワードの検査を行うべくステップ３に戻る。

【００５５】

ここで、図８に示すパスワード検査画面では、算出した得点および推定解析時間の他に、得点範囲に対応付けて定義される「弱すぎです」といったようなコメント情報や、これまでに入力したパスワードの中での得点順位を示す「４／６位」といったようなランキング情報や、パスワード候補生成ルーチン１１が最大生成可能とするパスワード候補の個数や、入力したパスワードとの一致が得られるまでに生成したパスワード候補の個数についても出力するという例を示している。

【００５６】

一方、ステップ１２の判断処理により、入力したパスワードとパスワード候補生成ルーチン１１から受け取ったパスワード候補とが一致しないことを判断する

ときには、ステップ１８に進んで、これまでに生成したパスワード候補の個数と、パスワード候補生成ルーチン１１が最大生成可能とするパスワード候補の個数とが一致したのか否かを判断して、一致しないことを判断するときには、次のパスワード候補を生成すべくステップ１０に戻る。

【００５７】

一方、ステップ１８の判断処理により、これまでに生成したパスワード候補の個数と、パスワード候補生成ルーチン１１が最大生成可能とするパスワード候補の個数とが一致したことを判断するときには、これ以上パスワード候補を生成することが不可能であるので、ステップ１３に進んで、上述の比率値ｔ（このルートを通る場合にはｔ＝１となる）を算出してから、ステップ１４～ステップ１７の処理を実行して、次のパスワードの検査を行うべくステップ３に戻る。

【００５８】

このようにして、パスワード強度検査プログラム１２は、検査対象のパスワードがブルートフォースの攻撃で用いられるパスワード推測ツールで生成される平文のパスワード候補の何個目のパスワードに該当するのかということを測定して、その何個目という数に従ってパスワードの強度を決定して出力するように処理するのである。

【００５９】

この実施形態例では、ユーザの属性情報としてユーザ名を入力させるようにして、入力されたユーザ名と入力されたパスワードとが一致する場合には、そのようなパスワードについては論外のパスワードであることを出力するように処理したが、電話番号や社員番号などのようなユーザ名以外のユーザの属性情報についても入力させるようにして、入力されたユーザ属性情報と入力されたパスワードとが一致する場合には、そのようなパスワードについては論外のパスワードであることを出力するように処理してもよい。

【００６０】

また、この実施形態例では、論外のパスワードについては順位テーブル１３に登録しないように処理したが、例えば、－１００点のような得点を割り当てて順位テーブル１３に登録するように処理してもよい。

【００６１】

【発明の効果】

以上説明したように、本発明では、検査対象のパスワードがブルートフォースの攻撃で用いられるパスワード推測ツールで生成される平文のパスワード候補の何個目のパスワードに該当するのかということを測定して、その何個目という数に従ってパスワードの強度を決定して出力するという構成を採ることから、実用的な時間内で数値的に表現されるパスワードの強度を算出できるようになることで、パスワードの強度を客観的かつ正確に検査できるようになる。

【００６２】

これから、本発明を用いることで、社員などに対して、どのようなパスワードが強いパスワードであるのかを客観的に教育できるようになることで、社内情報などのセキュリティを高めることができるようになる。

【図面の簡単な説明】

【図１】

本発明の一実施形態例である。

【図２】

順位テーブルの説明図である。

【図３】

パスワード強度検査プログラムの実行する処理フローの一実施形態例である。

【図４】

パスワード強度検査プログラムの実行する処理フローの一実施形態例である。

【図５】

パスワード検査画面の説明図である。

【図６】

パスワード検査画面の説明図である。

【図７】

パスワード検査画面の説明図である。

【図８】

パスワード検査画面の説明図である。

【図９】

パスワードに対して行われるブルートフォース攻撃の説明図である。

【符号の説明】

１　　パスワード強度検査装置

１０　入出力装置

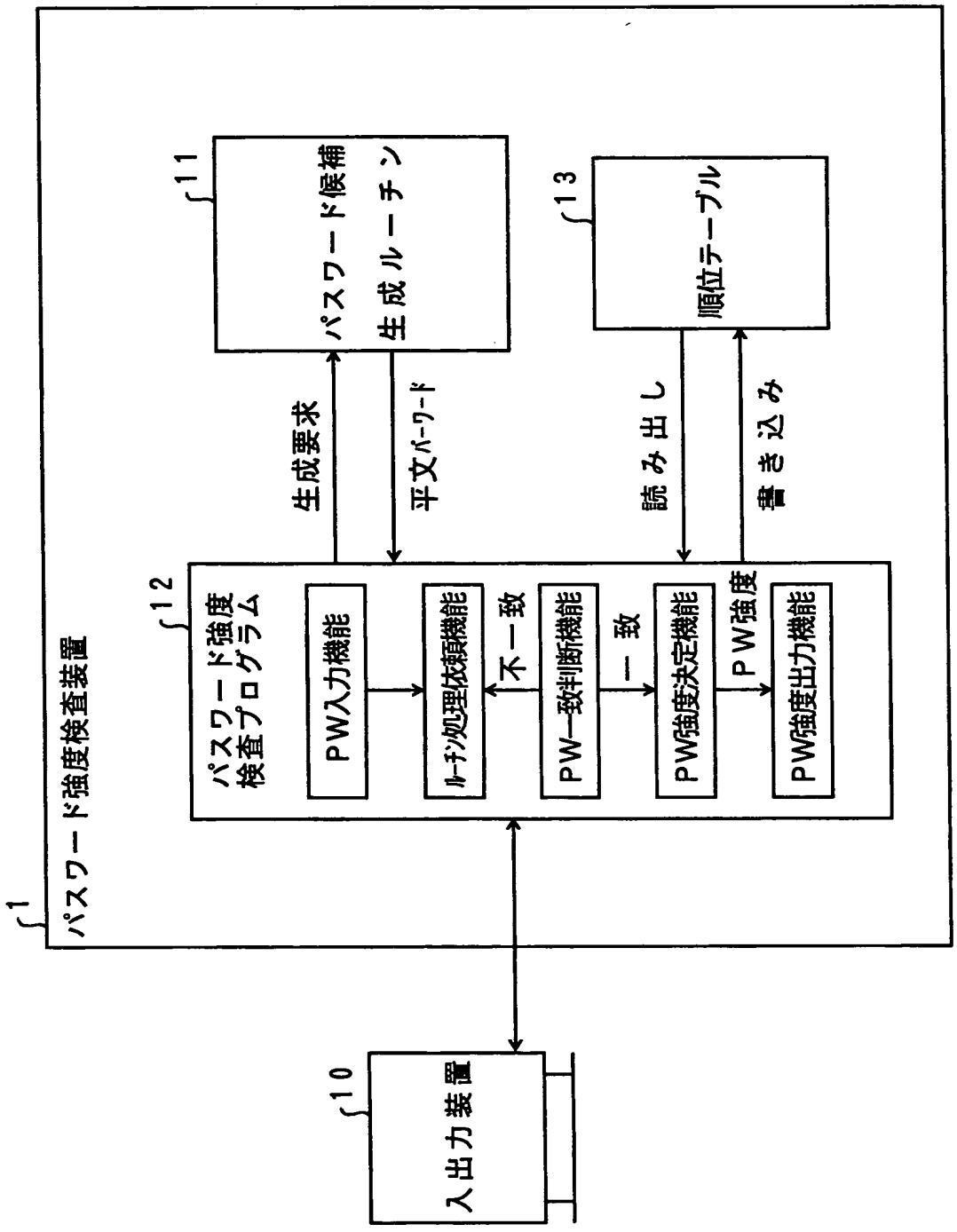
１１　パスワード候補生成ルーチン

１２　パスワード強度検査プログラム

１３　順位テーブル

【書類名】　図面

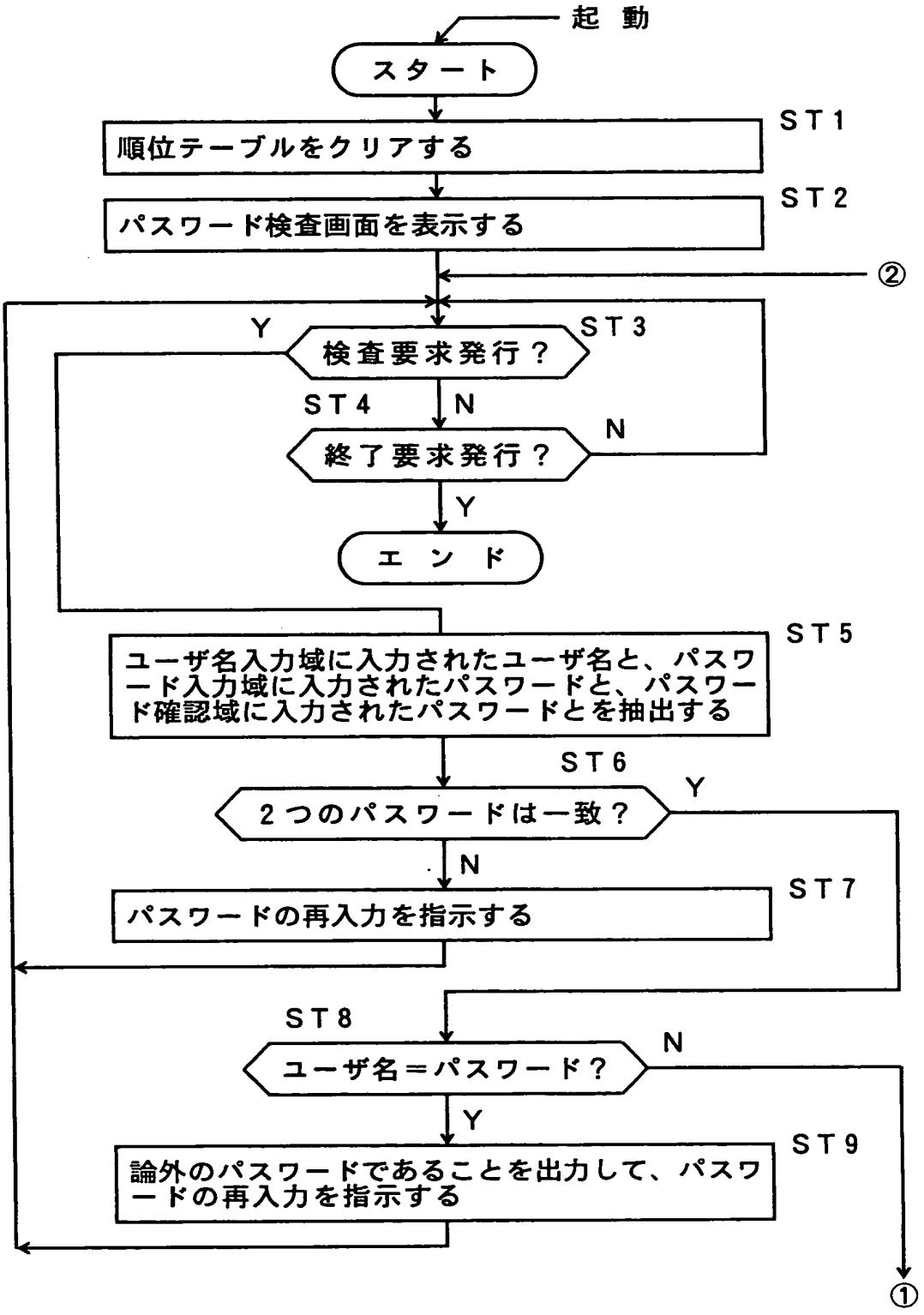
【図１】


1
パスワード強度検査装置
10
入出力装置
11
パスワード候補
生成ルーチン
12
パスワード強度
検査プログラム
PW入力機能
ルーチン処理依頼機能
PW一致判断機能
PW強度決定機能
PW強度出力機能
不一致
一致
PW強度
13
順位テーブル
生成要求
平文パスワード
読み出し
書き込み

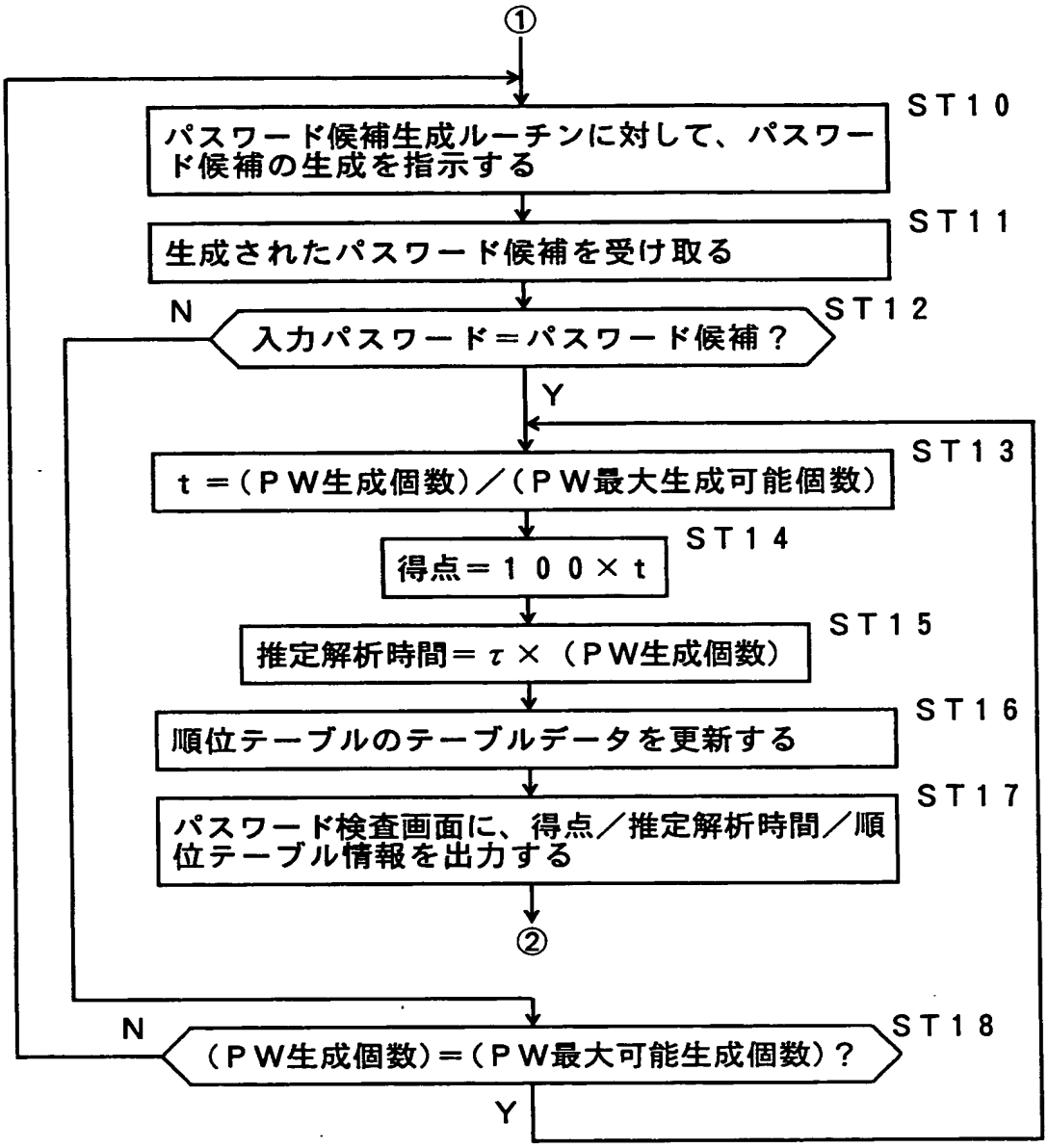
【図２】

順　位	ユーザ名	得　点	パスワード
1	××××××××××	６４点	□□□□□□□□□□
2	△△△△△△△△△△	４７点	○○○○○○○○○○
•	•	•	•
•	•	•	•
•	•	•	•
•	•	•	•
•	•	•	•
•	•	•	•
•	•	•	•
•	•	•	•
•	•	•	•
•	•	•	•
•	•	•	•

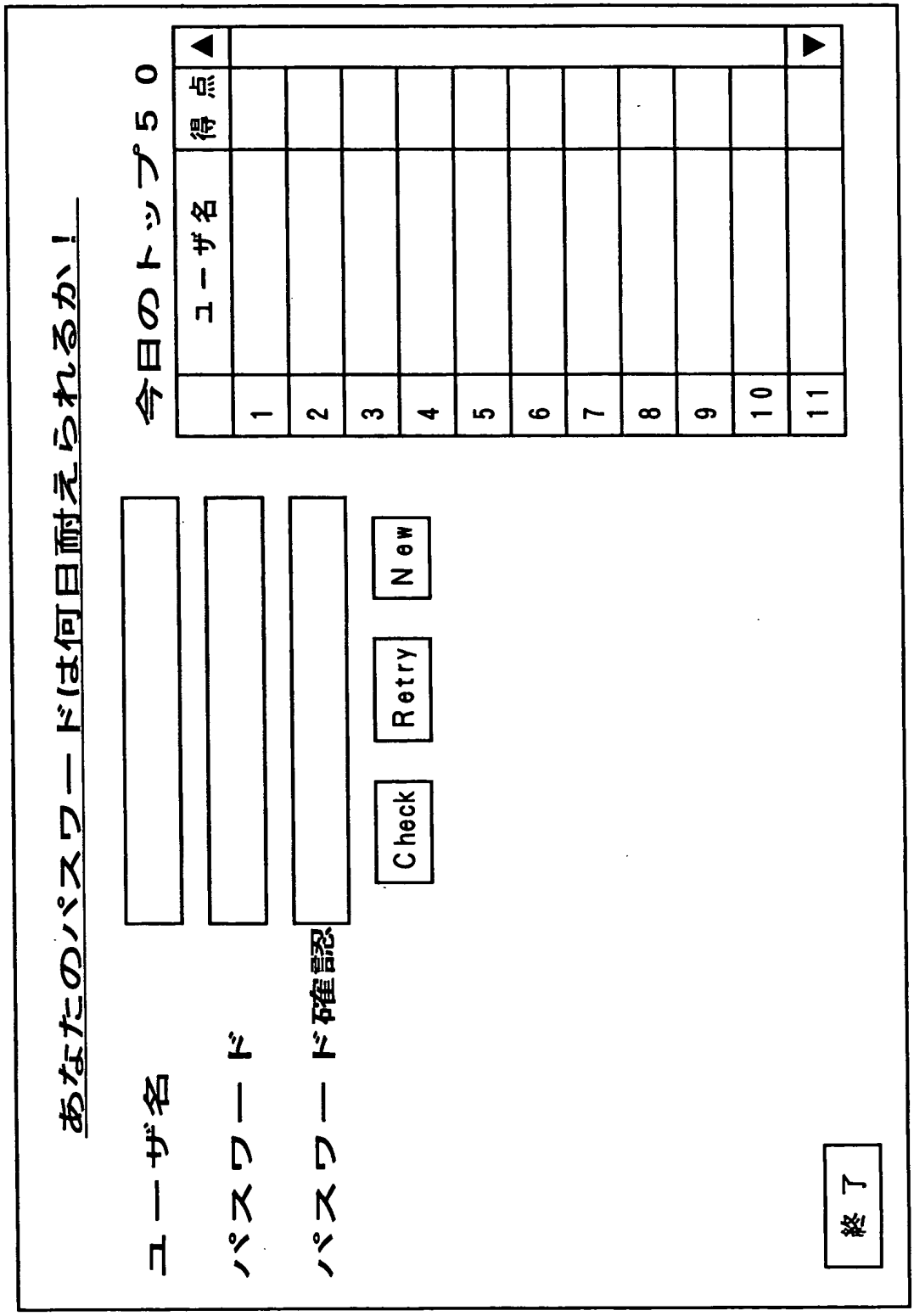
【図３】


起　動
スタート
ST１
順位テーブルをクリアする
ST２
パスワード検査画面を表示する
②
Y
ST３
検査要求発行？
ST４
N
N
終了要求発行？
Y
エ　ン　ド
ST５
ユーザ名入力域に入力されたユーザ名と、パスワード入力域に入力されたパスワードと、パスワード確認域に入力されたパスワードとを抽出する
ST６
Y
２つのパスワードは一致？
N
ST７
パスワードの再入力を指示する
ST８
N
ユーザ名＝パスワード？
Y
ST９
論外のパスワードであることを出力して、パスワードの再入力を指示する
①

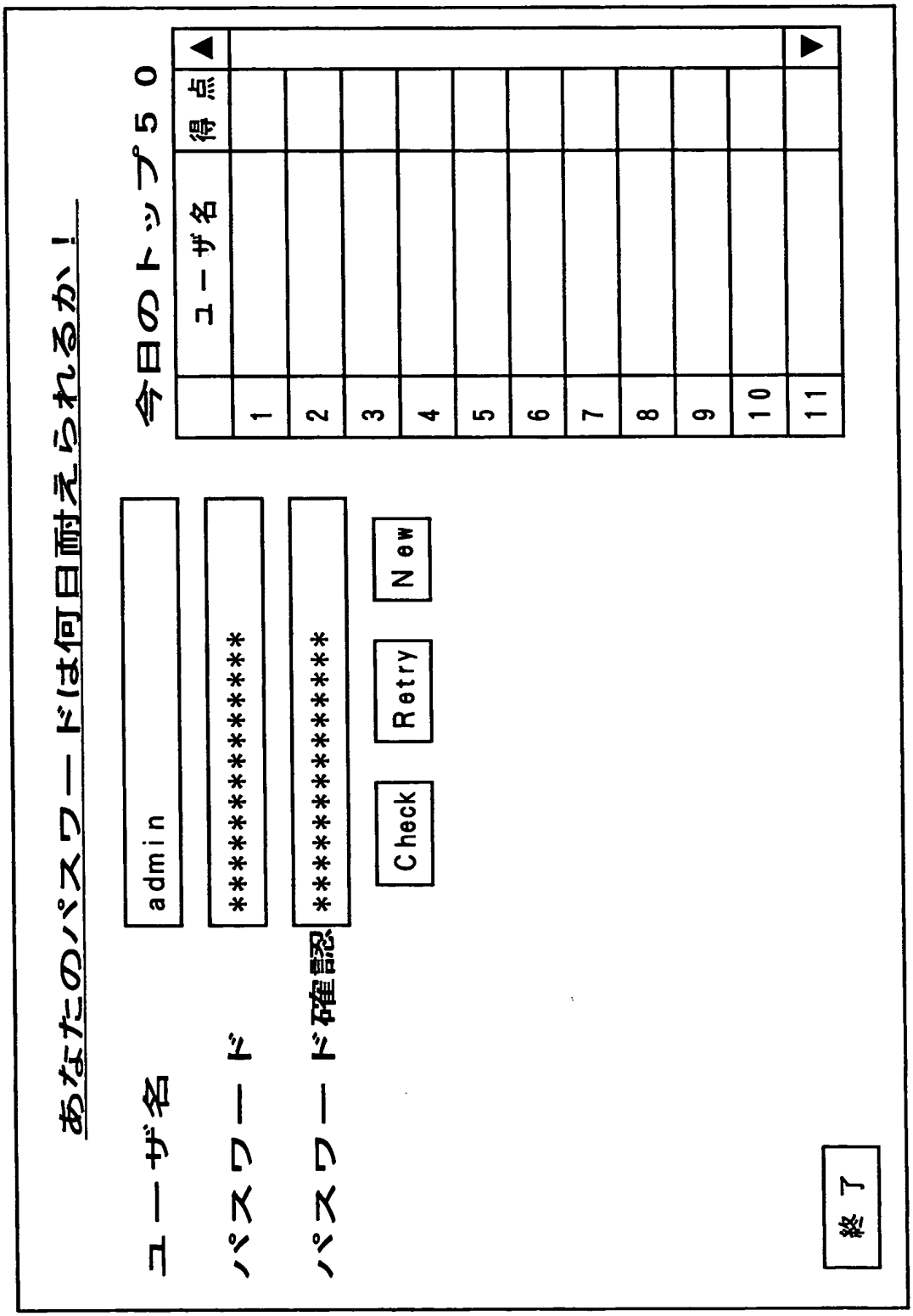
【図４】


①
ST１０
パスワード候補生成ルーチンに対して、パスワード候補の生成を指示する
ST１１
生成されたパスワード候補を受け取る
N
ST１２
入力パスワード＝パスワード候補？
Y
ST１３
t ＝（ＰＷ生成個数）／（ＰＷ最大生成可能個数）
ST１４
得点＝１００×t
ST１５
推定解析時間＝τ×（ＰＷ生成個数）
ST１６
順位テーブルのテーブルデータを更新する
ST１７
パスワード検査画面に、得点／推定解析時間／順位テーブル情報を出力する
②
N
ST１８
（ＰＷ生成個数）＝（ＰＷ最大可能生成個数）？
Y

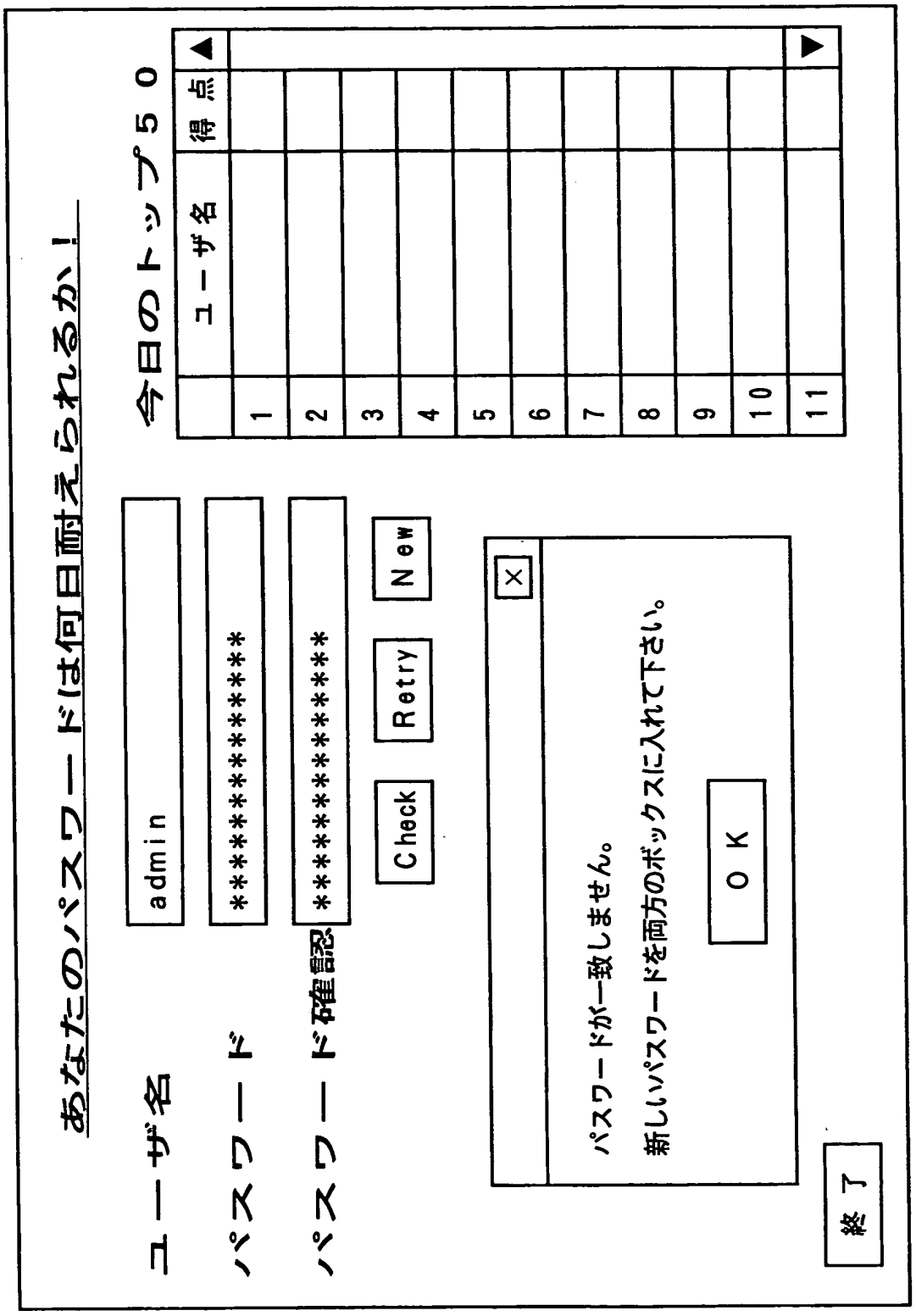
【図５】


あなたのパスワードは何日耐えられるか！
今日のトップ５０
ユーザ名
得点
1
2
3
4
5
6
7
8
9
10
11
ユーザ名
パスワード
パスワード確認
Check
Retry
New
終了

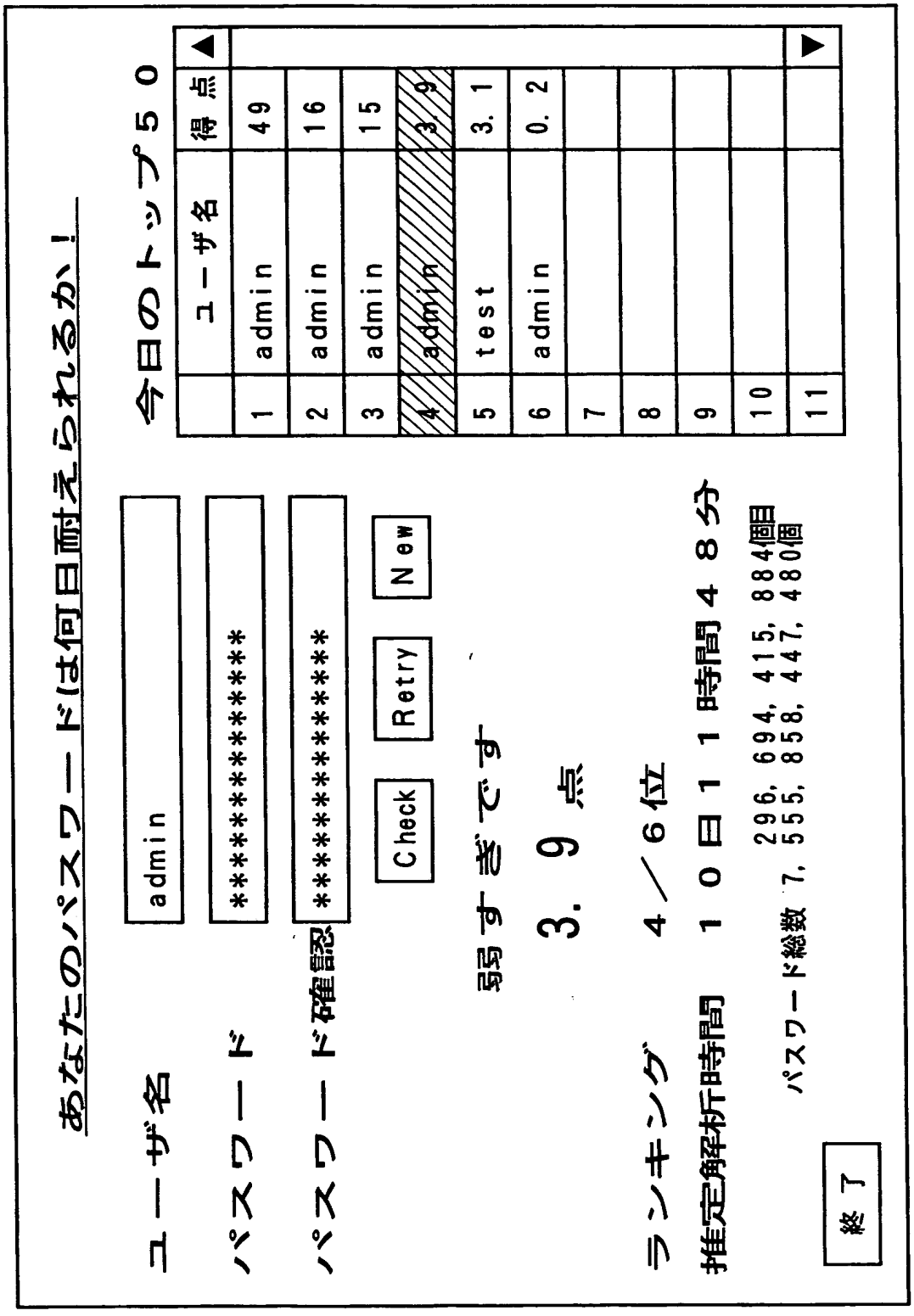
【図６】


あなたのパスワードは何日耐えられるか！
今日のトップ５０
ユーザ名
得点
1
2
3
4
5
6
7
8
9
10
11
ユーザ名
admin
パスワード
パスワード確認
Check
Retry
New
終了

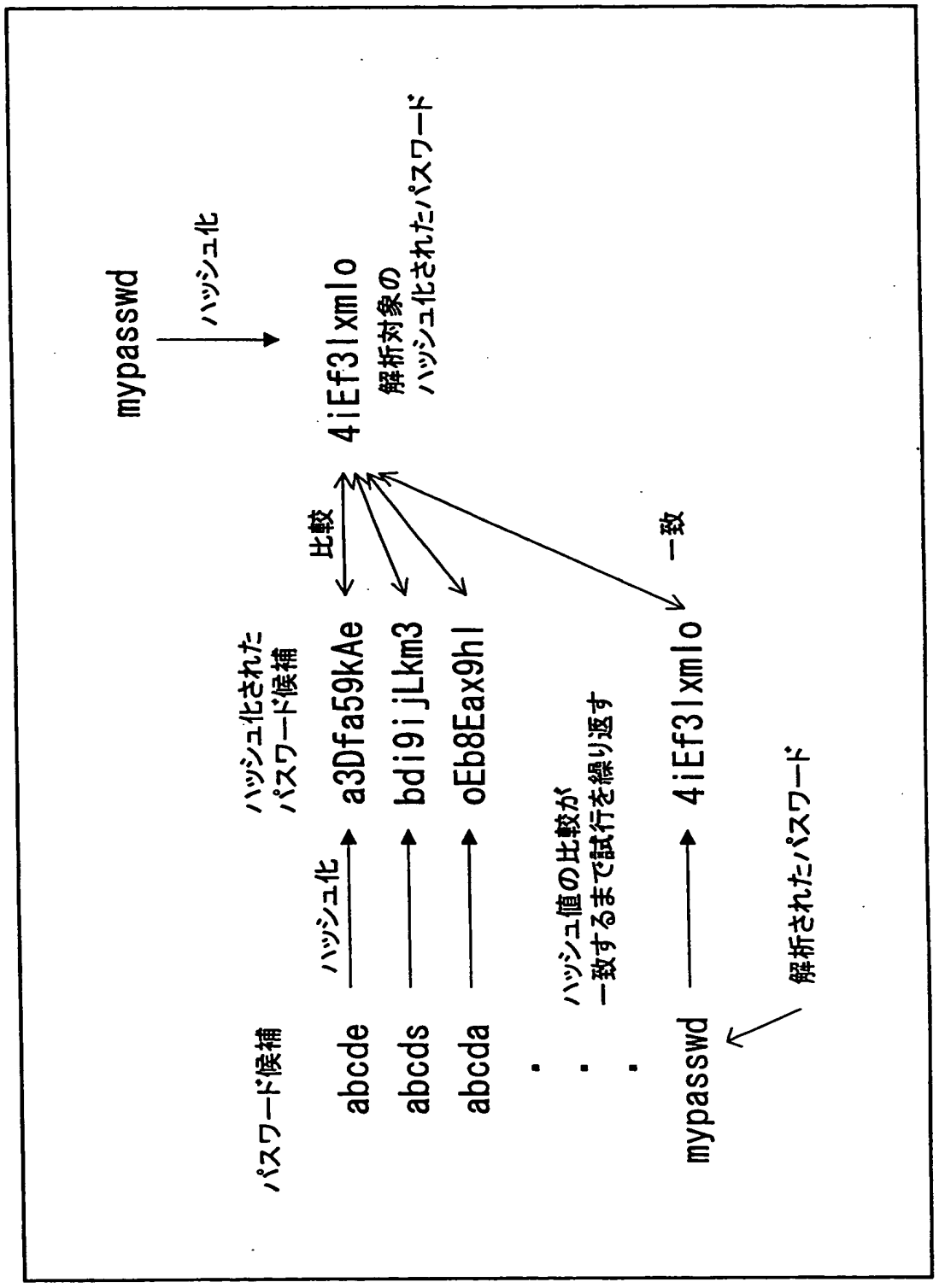
【図７】


あなたのパスワードは何日耐えられるか！
今日のトップ５０
ユーザ名
得点
1
2
3
4
5
6
7
8
9
10
11
ユーザ名
admin
パスワード
****
パスワード確認
****
Check
Retry
New
×
パスワードが一致しません。
新しいパスワードを両方のボックスに入れて下さい。
ＯＫ
終了

【図８】


あなたのパスワードは何日耐えられるか！
今日のトップ５０
ユーザ名
admin
パスワード
パスワード確認
Check
Retry
New
弱すぎです
3.9点
ランキング　４／６位
推定解析時間　１０日１１時間４８分
296,694,415,884個目
パスワード総数 7,555,858,447,480個
終了
ユーザ名
得点
1 admin 49
2 admin 16
3 admin 15
4 admin 3.9
5 test 3.1
6 admin 0.2
7
8
9
10
11

【図９】


mypasswd
ハッシュ化
4iEf3lxmlo
解析対象の
ハッシュ化されたパスワード
比較
一致
ハッシュ化された
パスワード候補
パスワード候補
ハッシュ化
a3Dfa59kAe
bdi9ijLkm3
oEb8Eax9hl
4iEf3lxmlo
abcde
abcds
abcda
mypasswd
ハッシュ値の比較が
一致するまで試行を繰り返す
解析されたパスワード

【書類名】　　要約書

【要約】

【課題】本発明は、パスワードの強度を客観的かつ正確に検査できるようにする新たなパスワード強度検査技術の提供を目的とする。

【解決手段】検査対象のパスワードを入力すると、パスワード推測ツールで用いられるものと同一の生成手順に従って、平文のパスワード候補を生成して、入力したパスワードと生成したパスワード候補とが一致するのか否かを判断する。そして、この一致を判断しない場合には、次のパスワード候補の生成を指示することで、入力したパスワードと生成したパスワード候補とが一致することになるまで、次々とパスワード候補を生成していく。一方、この一致を判断する場合には、生成したパスワード候補の個数に従って、入力したパスワードの強度を決定して、その決定したパスワード強度の情報を出力する。これにより、実用的な時間内で数値的に表現されるパスワードの強度を算出できるようになる。

【選択図】　　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００６６６６〕

１．変更年月日　　１９９８年　７月　１日
［変更理由］　名称変更
住　所　　東京都渋谷区渋谷２丁目１２番１９号
氏　名　　株式会社山武